

COUNTY COURT : COUNTY OF SUFFOLK
STATE OF NEW YORK

-----X

THE PEOPLE OF THE STATE OF NEW YORK,

Plaintiff,

- against -

ROBERT E. PRICE,

Defendant.

AFFIDAVIT IN SUPPORT
OF ORDER TO SHOW
CAUSE TO QUASH
SUBPOENA

Indictment No.: 1106-14

-----X

STATE OF WASHINGTON)
) SS.:
COUNTY OF KING)

Jacqueline F. Beauchere, being duly sworn, deposes and says:

1. I am the Chief Online Safety Officer ("COSO") at Microsoft Corporation ("Microsoft"). In this role, I am responsible for all aspects of Microsoft's online safety strategy, including cross-company policy creation and implementation, influence over consumer safety features and functionality, and communications to and engagement with a variety of external audiences. I have held this title for 22 months, and I have worked in online safety at Microsoft for more than 10 years. I have been at the company for 15 years, leading various groups and efforts that evangelize the company's commitment to help create a safer, more trusted Internet experience for people of all ages and abilities. I also currently serve as the chair of the National Cyber Security Alliance board of directors and am Microsoft's representative to the Family Online Safety Institute board of directors, as well as INHOPE's Advisory Board. This affidavit



is based on my own personal knowledge and on information to which I have access as COSO at Microsoft.

2. Microsoft has long viewed a safe online environment as a key selling point for its products and services. In 2002, Bill Gates, co-founder and then-chairman of Microsoft, called on employees to rethink their product development approach and strive to deliver products that are “as available, reliable and secure as standard services such as electricity, water services and telephony.” With that directive, Microsoft launched Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone based on sound business practices.

3. Microsoft’s work to keep individuals and families safer and more secure online has been part of that effort. Microsoft sees its responsibility in online safety as including technology tools for parents and caregivers, as well as providing public awareness-raising and educational materials to help inform the global public about online risks and how to mitigate them. For instance, Microsoft products such as Windows, Xbox 360, and Windows Phone are equipped with a number of family safety technology tools, such as restrictions on access to explicit content and download-blocking. These features are not legally required, but Microsoft has determined that many customers value such tools. In addition, the resources at Microsoft’s Safety & Security Center available online at <http://www.microsoft.com/security/default.aspx>, and its Family Safety Center at <http://www.microsoft.com/security/family-safety/default.aspx>, provide customers and the general public with information about protecting children from online bullying, ensuring that young people safely use social media, safeguarding online reputations and other issues related to personal and family online safety. Similarly, to protect the integrity of its services, Microsoft requires users to agree to a Code of Conduct that sets online community

standards, and Microsoft expressly reserves the right to remove content from its services, ban participants, and terminate services.

4. PhotoDNA is another element of Microsoft's voluntary business strategy to protect its customers, systems, and reputation by creating a safer online environment. PhotoDNA is an image-matching technology developed by Microsoft in collaboration with Dartmouth College that helps Microsoft find and remove images of child sexual abuse from Microsoft's online services.

5. Microsoft developed and implemented PhotoDNA as a result of its independent judgment that blocking illegal images of child sexual abuse from its services is in Microsoft's business interests. In Microsoft's experience, the direct and indirect costs resulting from the presence of such images on its services can be significant. For example, the presence of such images can increase the volume of consumer complaints received by Microsoft and, potentially, cause substantial harm to Microsoft's image and reputation in the marketplace. Microsoft believes that its customers are entitled to safer and more secure online experiences that are free of images depicting child sexual abuse. For these reasons, Microsoft devotes resources and develops and deploys technology, including PhotoDNA, to prevent the transmission and storage of images of child sexual abuse on Microsoft's services.

6. No government agency or law enforcement officer directed or requested that Microsoft create or use PhotoDNA.

7. PhotoDNA uses a mathematical algorithm to create a unique signature—similar to a fingerprint—for each digital image. It does this by adjusting the image to a standard size for processing; converting the image into black and white and breaking the image into sections; calculating a unique number to represent each section, and then placing all those

numbers together to create a single code that uniquely represents that image. That code is a unique signature for the digital image, which can be compared with the signatures of other images to find copies of the original image.

8. The technique described in the above paragraph is known as “hashing.” PhotoDNA’s robust hashing differs from other hashing technologies because the PhotoDNA signature is based on the essence of the image and not the specific electronic file containing the image. Therefore, if an image has been resized, recolored, saved in a different file format or otherwise similarly altered, PhotoDNA can still reliably identify copies of the image when other hashing technologies (that require every file characteristic to be precisely the same) could not.

9. Microsoft uses PhotoDNA on several of its services, including OneDrive (formerly known as SkyDrive), a cloud-based storage service, to scan certain user-generated content against a database of hashes of known images of child sexual abuse.

10. If the hash of scanned content matches the hash of a known image of child sexual abuse (also known as a “hit”), Microsoft takes several steps to prevent the continued access to and/or transmission of the images, to protect its customers, and to report the images as required by law. First, it suspends the account, such that the customer no longer has access to or use of the account or any other Microsoft online services associated with the account. Second, as required by federal law, Microsoft files a CyberTipline report with the National Center for Missing and Exploited Children (“NCMEC”). The report may contain basic information about the PhotoDNA match, including the file names, Internet Protocol (IP) address(es) associated with the account, and the name and email address that the customer provided when registering the account.

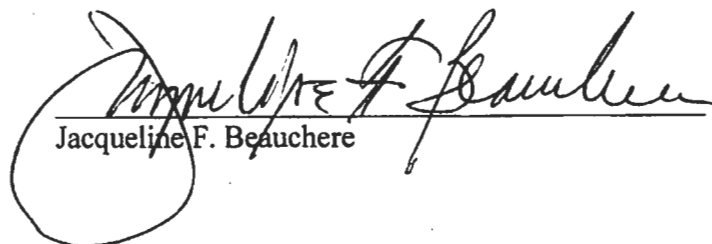
11. Robert Price ("Price") created his email address on Microsoft's Hotmail service, robprice987@hotmail.com, on March 9, 2013. At the same time the email account was created, Price automatically was provisioned a SkyDrive cloud storage account.

12. On October 30, 2013, PhotoDNA detected hits for three images stored on Price's SkyDrive account. Microsoft filed CyberTipline Report No. 2165115 to NCMEC on that day, reporting the three matches. The CyberTipline report contained Price's IP address, email address, screen name, and the file names of the three apparent PhotoDNA matches.

13. Microsoft conducted its own further investigation of Price's account on November 6, 2013. Microsoft did not conduct this further investigation at the direction or request of law enforcement or any government official, but rather solely to further its own business interests in keeping its services free of objectionable and/or illegal material. This further investigation identified 53 additional files on Price's SkyDrive account containing apparent images of child sexual abuse. As mandated by federal law, Microsoft then filed two additional CyberTipline reports, Nos. 2172540 and 2172566, on that day. The reports contained the IP address associated with Price's SkyDrive account, email address, screen name, and the file names of the suspected child pornography. With the reports, Microsoft also produced to NCMEC the 53 files containing the apparent images of child sexual abuse.

14. Neither NCMEC nor any government agency ever asked Microsoft to search any files associated with any of Price's Microsoft accounts, or assisted with any of Microsoft's investigation of Price's accounts, prior to Microsoft's filing of all three CyberTipline reports.

15. **Attachment A** contains the Terms of Service for SkyDrive that were in effect and applicable to Price on October 30, 2013, which incorporated Microsoft's Code of Conduct.


Jacqueline F. Beauchere

Sworn to before me this
30th day of January, 2015.



Notary Public

